

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-103048

(43)Date of publication of application : 13.04.2001

(51)Int.Cl.

H04L 9/32
G06F 12/14
G09C 5/00
H04N 1/387

(21)Application number : 11-273949

(71)Applicant : FUJITSU LTD

(22)Date of filing : 28.09.1999

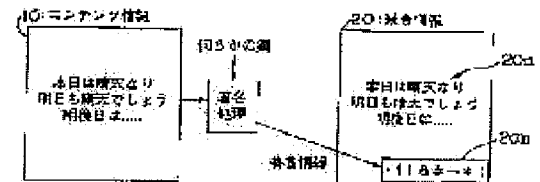
(72)Inventor : KOTANI MASATAKE
HASEBE TAKAYUKI
AKIYAMA RYOTA
SASAKI TAKAOKI

(54) METHOD AND DEVICE FOR MANAGING INFORMATION AND INFORMATION MANAGEMENT PROGRAM STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To give a sense of security that contents information is true to a user, about an information managing method or the like which manages digitized contents information.

SOLUTION: This information managing device generates signature information by subscribing one's name on the contents information 10 with a signature key, generates integrated information 20 obtained by uniting the contents information and the signature information into one and displays or outputs the form of the integrated information 20 as is, in the case of displaying or outputting the integrated information 20.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-103048

(P2001-103048A)

(43) 公開日 平成13年4月13日 (2001.4.13)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 L 9/32		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 9 C 5/00	5 C 0 7 6
G 0 9 C 5/00		H 0 4 N 1/387	5 J 1 0 4
H 0 4 N 1/387		H 0 4 L 9/00	6 7 3 D 9 A 0 0 1

審査請求 未請求 請求項の数17 O L (全 12 頁)

(21) 出願番号 特願平11-273949

(22) 出願日 平成11年9月28日 (1999.9.28)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 小谷 誠剛

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72) 発明者 長谷部 高行

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74) 代理人 100094330

弁理士 山田 正紀

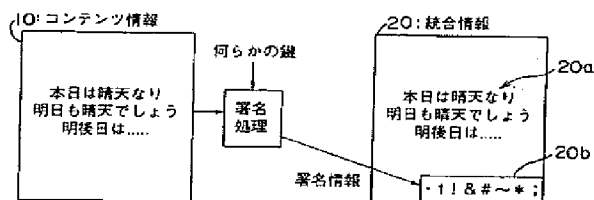
最終頁に続く

(54) 【発明の名称】 情報管理方法、情報管理装置、および情報管理プログラム記憶媒体

(57) 【要約】

【課題】本発明は、デジタル化されたコンテンツ情報を管理する情報管理方法等に関し、コンテンツ情報が真正なものであるという安心感をユーザに与える。

【解決手段】コンテンツ情報10を署名鍵で署名して署名情報を生成し、そのコンテンツ情報と署名情報を一体化した統合情報20を生成し、表示やプリント出力にあたっては、その統合情報20の形態のまま表示あるいは出力を行なう。



【特許請求の範囲】

【請求項 1】 コンテンツ情報に署名鍵で署名することにより署名情報を生成し、

該コンテンツ情報と該署名情報を、視覚的に一体化された統合情報に統合することを特徴とする情報管理方法。

【請求項 2】 所定の秘密情報に基づいて署名鍵を生成し、この生成された署名鍵でコンテンツ情報に署名することを特徴とする請求項 1 記載の情報管理方法。

【請求項 3】 所定の可視情報を二次元ビットマップに変換することにより二次元情報を生成し、この生成された二次元情報と所定の秘密情報とに基づいて署名鍵を生成し、この生成された署名鍵でコンテンツ情報に署名することを特徴とする請求項 1 記載の情報管理方法。

【請求項 4】 前記可視情報が手書きされた情報であることを特徴とする請求項 3 記載の情報管理方法。

【請求項 5】 前記可視情報が押印された情報であることを特徴とする請求項 3 記載の情報管理方法。

【請求項 6】 コンテンツ情報への署名に代えて、コンテンツ情報に所定の付加情報を付加した情報に署名鍵で署名し、該コンテンツ情報と該署名鍵とさらに該付加情報とを統合することによって、視覚的に一体化された統合情報を生成することを特徴とする請求項 1 記載の情報管理方法。

【請求項 7】 コンテンツ情報に時刻情報を付加し、時刻情報が付加されたコンテンツ情報に署名鍵で署名することを特徴とする請求項 1 記載の情報管理方法。

【請求項 8】 前記統合情報からコンテンツ情報と署名情報を分離するとともに、該統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報を生成し、この生成された検証用署名情報と、前記統合情報から分離された署名情報とを比較することを特徴とする請求項 1 記載の情報管理方法。

【請求項 9】 所定の秘密情報に基づいて署名鍵を生成し、この生成された署名鍵で、前記統合情報から分離されたコンテンツ情報に署名することを特徴とする請求項 8 記載の情報管理方法。

【請求項 10】 所定の可視情報を二次元ビットマップに変換することにより二次元情報を生成し、この生成された二次元情報と所定の秘密情報とに基づいて署名鍵を生成し、この生成された署名鍵で、前記統合情報から分離されたコンテンツ情報に署名することを特徴とする請求項 8 記載の情報管理方法。

【請求項 11】 前記統合情報から分離された署名情報と、該統合情報から分離されたコンテンツ情報に署名鍵で署名することにより得られた検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、該統合情報へのアクセスを許容することを特徴とする請求項 8 記載の情報管理方法。

【請求項 12】 コンテンツ情報に署名鍵で署名することにより署名情報を生成する署名手段と、

前記署名手段により署名されたコンテンツ情報と該署名により生成された署名情報を、視覚的に一体化された統合情報に統合する統合手段とを備えたことを特徴とする情報管理装置。

【請求項 13】 前記統合情報からコンテンツ情報と署名情報を分離する分離手段と、該統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報を生成する検証用署名手段と、

該検証用署名手段で生成された検証用署名情報と、前記分離手段により前記統合情報から分離された署名情報とを比較する比較手段とを備えたことを特徴とする請求項 12 記載の情報管理装置。

【請求項 14】 前記比較手段は、前記分離手段により前記統合情報から分離された署名情報と、前記検証用署名手段により生成された検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、該統合情報へのアクセスを許容するものであることを特徴とする請求項 13 記載の情報管理装置。

【請求項 15】 コンテンツ情報に署名鍵で署名することにより署名情報を生成する署名手段と、

前記署名手段により署名されたコンテンツ情報と該署名により生成された署名情報を、視覚的に一体化された統合情報に統合する統合手段とを有する情報管理プログラムが記憶されていることを特徴とする情報管理プログラム記憶媒体。

【請求項 16】 前記情報管理プログラムは、前記統合情報からコンテンツ情報と署名情報を分離する分離手段と、

該統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報を生成する検証用署名手段と、該検証用署名手段で生成された検証用署名情報と、前記分離手段により前記統合情報から分離された署名情報とを比較する比較手段とを、さらに有するものであることを特徴とする請求項 15 記載の情報管理プログラム記憶媒体。

【請求項 17】 前記比較手段は、前記分離手段により前記統合情報から分離された署名情報と、前記検証用署名手段により生成された検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、該統合情報へのアクセスを許容するものであることを特徴とする請求項 16 記載の情報管理プログラム記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル化されたコンテンツ情報を管理する情報管理方法、情報管理装置、および、コンピュータあるいはコンピュータシステムをそのような情報管理装置として機能させるための情報管理プログラムが記憶された情報管理プログラム記憶

媒体に関する。

【0002】

【従来の技術】コンテンツ情報のデジタル化が時代の趨勢となってきた。デジタル化されたコンテンツ情報に署名鍵でデジタル署名を行ない署名情報を生成することが容易になり、その署名情報をコンテンツ情報に対応づけて運用することが盛んに行なわれるようになってきている。

【0003】デジタル署名によって生成される署名情報はコンテンツ情報に依存した情報であり、異なるコンテンツ情報からは異なる署名情報が生成される。例えば修正あるいは改ざんされたコンテンツ情報にデジタル署名を行なったとき、生成される署名情報がその修正あるいは改ざんによってどのように変化するかを予想することは極めて困難である。この性質を利用し、例えばそのコンテンツ情報と署名情報を送信して、それらを受信した側でその受信したコンテンツ情報を同じ署名鍵で再度署名して署名情報を生成し、その生成した署名情報と受信した署名情報とを比較することにより、そのコンテンツ情報が修正あるいは改ざんのない真正なものであるかどうかを調べることができる。

【0004】

【発明が解決しようとする課題】コンテンツ情報の修正や改ざんの有無の検出自体については、上記のような署名情報を用いることによって可能であるが、この検出作業はコンピュータ等の内部のユーザからは見えない部分で行なわれるため、修正や改ざんのない、確かに真正なコンテンツ情報であるという安心感をユーザに与えにくいという、感覚的な面で問題がある。

【0005】古来、印影や手書きサインで本人認証をしてきた長い歴史がありそれが文化として確立している中では、コンピュータ等の内部で自分には見えないところで処理されてこれは真正なものであるという結果だけ情報を与えられることに對し違和感を抱く人々が多数存在することも否定できない。

【0006】手書き文字（サイン）を入力してその手書き文字を基に署名鍵を作成することが提案されており

（特開平7-262372号公報参照）、これを採用すると、コンテンツ情報を作成した側にそのコンテンツ情報に確かに署名したという一種の安心感を与える効果はあるが、そのコンテンツ情報を利用する側における、そのコンテンツ情報が真正なものであるという納得がいま一つ十分でないという問題点を解決するものではない。

【0007】本発明は、上記事情に鑑み、コンテンツ情報が真正なものであるという安心感をユーザに与えることのできる情報管理を実現する情報管理方法、その情報管理方法を実行する情報管理装置、および、コンピュータあるいはコンピュータシステムで実行されることによりそのような情報管理を実現する情報管理プログラムが記憶された情報管理プログラム記憶媒体を提供すること

を目的とする。

【0008】

【課題を解決するための手段】上記目的を達成する本発明の情報管理方法は、コンテンツ情報に署名鍵で署名することにより署名情報を生成し、そのコンテンツ情報とその署名情報を、視覚的に一体化された統合情報に統合することを特徴とする。

【0009】ここで、上記の「視覚的に一体化された」とは、画面表示や用紙上へのプリント出力の際に、一体化された情報として表示ないし出力されることをいう。典型的にはそのコンテンツ情報と署名情報が一体的に1つのファイルに格納されていることをいうが、コンテンツ情報と署名情報が別々のファイルを構成し、画面表示あるいはプリント出力にあたってひとかたまりの情報として表示ないし出力されるように構成したものであってもよい。

【0010】本発明の情報管理方法によれば、コンテンツ情報と署名情報が、例えば表示画面上への表示あるいは用紙上へのプリント出力等の場合に、視覚的に一体化された統合情報に統合されているため、その統合情報として一体化された署名情報が、心理上、長い歴史の中で培ってきた印影やサインと同様の役割りを果たし、ユーザに安心感を与えることができる。

【0011】また、コンテンツ情報は表示画面上でのみ確認する場合も多いが、そのコンテンツ情報が重要な情報であればあるほど用紙上にプリント出力してそのコンテンツ情報を保存しあるいは利用することも多い。そのような場合、本発明によれば、用紙上にコンテンツ情報のみでなく署名情報も記録されているためそのコンテンツ情報が真正なものであることを確認する必要を生じたときはその用紙上の記録をOCR（光学的な文字入力装置）により読み込ませその読み込ませた統合情報から署名情報を分離して検証に用いることができる。実際にはプリント出力された全てのものについて上記のようなOCRで読み込ませて検証するという作業を行なわなくても、プリント出力されたものからも真正であることを検証する方が存在するというところをもってユーザに大きな安心感を与えることができる。

【0012】ここで、上記本発明の情報管理方法において、所定の秘密情報に基づいて署名鍵を生成し、この生成された署名鍵でコンテンツ情報に署名することが好ましい。

【0013】上記の「所定の秘密情報」は、特定のものに限られるものではないが、典型的には、この情報管理方法の実施がある1台のコンピュータ内で完結しているときはそのコンピュータにユニークな装置番号等を行い、あるいは、この情報管理方法がある1つのシステムに加入している加入者間で共用されるときはそのシステムの加入者にのみ通知されるパスワード等をいう。

【0014】このように、署名情報の生成時に使用する

署名鍵を、システムあるいは装置の秘密情報から生成することにより、同一のコンテンツ情報を別システムあるいは別装置にて処理する場合において署名情報を異なるものとすることができ、したがって署名情報のユニーク性を高めることができる。

【0015】また、上記本発明の情報管理方法において、所定の可視情報を二次元ビットマップに変換することにより二次元情報を生成し、この生成された二次元情報と所定の秘密情報とに基づいて署名鍵を生成し、この生成された署名鍵でコンテンツ情報に署名することも好ましい態様である。ここで、上記可視情報は手書きされた情報であってもよく、あるいは、上記可視情報は押印された情報であってもよく、その他の可視情報（例えばあるシステムの加入者あるいはあるグループの構成員であることを表わすマークや文字等）であってもよい。

【0016】このように、秘密情報に加えて可視情報から作成された二次元情報を用いて署名鍵を生成すると署名情報のユニーク性を一層高めることができる。この場合において、手書きされた情報や押印された情報を可視情報として使用すると、従来から慣習として行なわれてきた手書きサイン認証や捺印認証と親和性のある署名認証を行なうことができる。

【0017】さらに、上記本発明の情報管理方法において、コンテンツ情報への署名に代えて、コンテンツ情報に所定の付加情報を付加した情報に署名鍵で署名し、そのコンテンツ情報とその署名鍵とさらにその付加情報とを統合することによって、視覚的に一体化された統合情報を生成することも好ましい。

【0018】この「付加情報」は特定の情報に限定されるものではないが、例えば署名時点における時刻情報、あるいは作成されたコンテンツ情報の内容を承認した承認者（例えば会社におけるある部署の責任者）の名前等であってもよい。

【0019】このように、コンテンツ情報に、そのコンテンツ情報とは別の概念としての付加情報を付加して署名することにより、コンテンツ情報に署名した時刻や承認者名等を明確にすることができ、また、後の署名照合等においてその付加情報を運用することができる。

【0020】また、上記本発明の情報管理方法において、コンテンツ情報に時刻情報を付加し、時刻情報が付加されたコンテンツ情報に署名鍵で署名することも好ましい形態である。

【0021】この「時刻情報」は特定のものに限られるものではなく、例えばコンテンツ情報作成時の時刻を表わす時刻情報であってもよく、あるいは署名時の時刻であってもよい。

【0022】このようにコンテンツ情報に時刻情報を付加しその時刻情報が付加された情報をコンテンツ情報として取り扱うことによっても、上述のコンテンツ情報とは別に付加情報を付加する場合と同様、そのコンテンツ

情報の作成時刻あるいは署名時刻を明確にすることができる。

【0023】さらに、本発明の情報管理方法において、コンテンツ情報が真正のものであるかどうか検証する必要があるときは、上記統合情報からコンテンツ情報と署名情報を分離するとともに、その統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報が生成され、この生成された検証用署名情報と、上記統合情報から分離された署名情報とが比較される。

【0024】本発明では、署名情報が人の目に見える形でコンテンツ情報と統合されて統合情報となっているため、署名照合の処理に用いられる情報を把握することが容易であり、かつ、上記のようにしてコンテンツ情報が真正なものであることを検証する方法を確立しておくことにより、ユーザの安心感が一層高められる。

【0025】さらに、この検証時においても、所定の秘密情報に基づいて署名鍵を生成し、この生成された署名鍵で、上記統合情報から分離されたコンテンツ情報に署名することが好ましく、所定の可視情報を二次元ビットマップに変換することにより二次元情報を生成し、この生成された二次元情報と所定の秘密情報とに基づいて署名鍵を生成し、この生成された署名鍵で、上記統合情報から分離されたコンテンツ情報に署名することがさらに好ましい。

【0026】システムまたは装置の秘密情報から署名鍵を生成することにより、あるいはその秘密情報と、可視情報から作成された二次元情報とから署名鍵を作成することにより、前述したように、署名情報のユニーク性を高めることができる。

【0027】ここで、統合情報から分離された署名情報と、その統合情報から分離されたコンテンツ情報に署名鍵で署名することにより得られた検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、その統合情報へのアクセスを許容することにより、改ざんあるいはデータエラーの可能性のあるコンテンツ情報へのアクセスを防止することができる。

【0028】また、上記目的を達成する本発明の情報管理装置は、コンテンツ情報に署名鍵で署名することにより署名情報を生成する署名手段と、その署名手段により署名されたコンテンツ情報とその署名により生成された署名情報を、視覚的に一体化された統合情報に統合する統合手段とを備えたことを特徴とする。

【0029】この情報管理装置において、さらに上記統合情報からコンテンツ情報と署名情報を分離する分離手段と、その統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報を生成する検証用署名手段と、検証用署名手段で生成された検証用署名情報と、分離手段により統合情報から分離された署名情報とを比較する比較手段とを備えたことを特徴とす

る。

【0030】この場合に、上記比較手段は、分離手段により統合情報から分離された署名情報と、検証用署名手段により生成された検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、その統合情報へのアクセスを許容するものであることが好ましい。

【0031】また、上記目的を達成する本発明の情報管理プログラム記憶媒体は、コンテンツ情報に署名鍵で署名することにより署名情報を生成する署名手段と、その署名手段により署名されたコンテンツ情報とその署名により生成された署名情報を、視覚的に一体化された統合情報に統合する統合手段とを有する情報管理プログラムが記憶されていることを特徴とする。

【0032】この情報管理プログラムは、上記統合情報からコンテンツ情報と署名情報を分離する分離手段と、その統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報を生成する検証用署名手段と、その検証用署名手段で生成された検証用署名情報と、分離手段により統合情報から分離された署名情報とを比較する比較手段とを、さらに有するものであることが好ましい。

【0033】この場合に、上記比較手段は、分離手段により統合情報から分離された署名情報と、検証用署名手段により生成された検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、その統合情報へのアクセスを許容するものであることが好ましい。

【0034】尚、本発明の情報管理装置と本発明の情報管理プログラム記憶媒体に記憶された情報管理プログラムとの双方で「手段」という用語を用いているが、情報管理装置における手段は、ハードウェアとソフトウェアとの組合せをいい、情報管理プログラムの場合は、そのうちのソフトウェアの部分のみを手段と称している。

【0035】

【発明の実施の形態】以下、本発明の実施形態について説明する。

【0036】図1は、本発明の情報管理装置の一実施形態を構成するパーソナルコンピュータの外観斜視図である。このパーソナルコンピュータには、本発明という情報管理プログラムの一実施形態がインストールされて実行されることにより、本発明の一実施形態としての情報管理方法が実施される。

【0037】このパーソナルコンピュータ100は、CPU、RAM、ハードディスク等を内蔵した本体部101、本体部101からの指示により表示画面102aに画面表示を行うCRTディスプレイ102、このパーソナルコンピュータにユーザの指示や文字情報を入力するためのキーボード103、表示画面102a上の任意の位置を指定することによりその位置に表示されていたアイコン等に応じた指示を入力するマウス104を備えている。

【0038】本体部101は、さらに、外観上、フロッピーディスク212（図1には図示せず；図2参照）やCDROM210が取り出し自在に装填されるフロッピーディスク装填口101aおよびCDROM装填口101bを有しており、その内部には、装填されたフロッピーディスクやCDROM210をドライブする、フロッピーディスクドライバ224、CDROMドライバ225（図2参照）も内蔵されている。

【0039】ここでは、CDROM210に、本発明という情報管理プログラムの一例が記憶されている。このCDROM210がCDROM装填口101bから本体部101内に装填され、CDROMドライバ225により、そのCDROM210に記憶された情報管理プログラムがこのパーソナルコンピュータ100のハードディスク内にインストールされる。

【0040】この情報管理プログラムが記憶されたCDROMは、本発明の情報管理プログラム記憶媒体の一実施形態に相当する。

【0041】また、このCDROMに記憶された情報管理プログラムは、上記のようにしてパーソナルコンピュータ100のハードディスク内にインストールされるが、その情報管理プログラムがインストールされた状態のハードディスクも、本発明の情報管理プログラム記憶媒体の一実施形態に相当する。

【0042】さらに、その情報管理プログラムがフロッピーディスク等にダウンロードされるときは、そのダウンロードされた情報管理プログラムを記憶した状態にあるフロッピーディスク等も、本発明の情報管理プログラム記憶媒体の一実施形態に相当する。

【0043】図2は、図1に外観を示すパーソナルコンピュータのハードウェア構成図である。

【0044】ここには、中央演算処理装置（CPU）221、RAM222、ハードディスクコントローラ223、フロッピーディスクドライバ224、CDROMドライバ225、マウスコントローラ226、キーボードコントローラ227、およびディスプレイコントローラ228が示されており、それらはバス220で相互に接続されている。

【0045】フロッピーディスクドライバ224、CDROMドライバ225は、図1を参照して説明したように、それぞれフロッピーディスク212、CDROM210が装填され、装填されたフロッピーディスク212、CDROM210をアクセスするものである。

【0046】図3は、CDROMに記憶された情報管理プログラムの一例を示す図である。

【0047】この図3に示すように、CDROM210は、署名手段251、統合手段252、分離手段253、検証用署名手段254、および比較手段255を有する情報管理プログラム250が記憶されている。各手段221～225の詳細については後述する。

【0048】図4は、本発明にいう情報管理プログラムが動作するもう1つの環境であるコンピュータネットワークを示す図である。

【0049】この図4には、コンピュータネットワークを構成するコンピュータシステムとして2台のクライアントマシン300、400と1台のサーバマシン500が例示されており、これらのコンピュータシステム300、400、500は通信網600を介して互いに接続されている。

【0050】各クライアントマシン300、400およびサーバマシン500は、基本的には図1、図2に示すパーソナルコンピュータに通信の機能を付加した構成を備えている。すなわち、各クライアントマシン300、400およびサーバマシン500は、CPU、主記憶装置、ハードディスク、通信用ボード等が内蔵された本体部301、401、501、本体部301、401、501からの指示により表示画面302a、402a、502a上に画像や文字列を表示する表示部302、402、502、本体部301、401、501にユーザの指示を入力するためのキーボード303、403、503、表示画面302a、402a、502a上の任意の位置を指定することにより、その指定時にその位置に表示されていたアイコン等に応じた指示を入力するマウス304、404、504を備えている。

【0051】また、各本体部301、401、501には、さらに外観上、フロッピディスクが装填されるFD装填口301a、401a、501a、CDROM装填口301b、401b、501bを有しており、それらの内部には、それらの装填口301a、301b；401a、401b；501a、501bから装填されたフロッピディスクやCDROMをドライブしてアクセスする、フロッピディスクドライブ、CDROMドライブも内蔵されている。

【0052】サーバマシン500は、クライアントマシン300、400のホストコンピュータとして働き、クライアントマシン300、400間で送受信される電子メール等のコンテンツ情報の送受信を仲介する。

【0053】以下、図1に示すパーソナルコンピュータ内部、あるいは図4に示すコンピュータネットワーク内で実行される、本発明に沿った処理について説明する。ここでは、図1に示すパーソナルコンピュータを動作環境とする場合は、コンテンツ情報に署名して統合情報を生成する第1段階と、その統合情報中のコンテンツ情報が真正なものであるか否か検証を行なう第2段階との双方がそのパーソナルコンピュータで実行され、図4に示すコンピュータネットワークを動作環境とする場合は、上記の態様のほか、上述の第1段階はクライアントマシン300、400のうちのコンテンツ情報送信側のマシンで実行され、上述の第2段階はそれらのクライアントマシン300、400のうちの受信側のマシンで実行さ

れるという態様も存在する。

【0054】図5は、統合情報生成処理の第1例を示す模式図、図6は、その統合情報生成処理を表わすフローチャートである。

【0055】ここでは先ずコンテンツ情報10の入行が行なわれる（ステップS1）。コンテンツ情報の入手は、コンテンツ情報を新たに作成したりあるいは既に存在するコンテンツ情報を新たに修正あるいは編集して作成したものであってもよく、あるいは外部で作成されたコンテンツ情報を入手したものであってもよい。

【0056】次にそのコンテンツ情報10に署名するための署名鍵の入手が行なわれる（ステップS2）。この署名鍵は、既に記憶しておいたものを読み出してもよく、あるいはユーザによりパスワード等として入力されるものであってもよく、ここではその署名鍵の入手方法の如何を問うものではない。

【0057】上記のようにコンテンツ情報と署名鍵が入手された後、そのコンテンツ情報10にその署名鍵で署名処理が行なわれて署名情報が生成される（ステップS3）。この署名処理は、図3に示す情報処理プログラム250の署名手段251に相当する。

【0058】次に、その生成された署名情報をコンテンツ情報と統合して統合情報20を生成する（ステップS4）。この統合情報20は、本発明で要請される要件としては、表示やプリント出力のときにコンテンツ情報と署名情報が視覚的に一体化されていればよいが、本実施形態では、表示や出力のときのみでなく、コンテンツ情報20aと署名情報20bが全体として1つの情報として常に一体化された1つのファイルが作成される。この統合処理（ステップS4）は、図3に示す情報処理プログラム250における統合手段252に相当する。

【0059】このようにコンテンツ情報と署名情報を一体化した統合情報を作成することにより、その統合情報中の署名情報が印影やサインと同様の役割りを果たし、ユーザに安心感を与えることができる。

【0060】図7は、統合情報生成処理の第2例を示す模式図、図8は、その第2例を実現するための、図6に示すフローチャートからの変更部分を示す部分フローチャートである。

【0061】図7において図5と異なる点は、コンテンツ情報10に署名処理を行なうための署名鍵が、システム又は装置内の秘密情報から作成されるものであるという点が明示されている点である。

【0062】この場合、図8に示すように、図6の鍵入手のステップS2は、秘密情報入手のステップ201とその秘密情報に基づいて署名鍵を生成するステップS202で構成される。秘密情報としては、図1に示す動作環境の場合はそのパーソナルコンピュータの装置番号、図4に示す動作環境の場合はそのコンピュータネットワークにユニークなパスワード等を採用することができ

る。

【0063】このように署名鍵を秘密情報に基づいて作成することにより、その署名鍵を用いて生成される署名情報のユニーク性を高めることができる。

【0064】図9は、統合情報生成処理の第3例を示す模式図、図10は、その第3例を実現するための、図6に示すフローチャートからの変更部分を示す部分フローチャートである。

【0065】図9において図5とは異なる点は、可視情報が二次元処理により二次元のビットマップを表わす二次元情報に変換され、その二次元情報と秘密情報とに基づいて署名鍵が作成される点である。

【0066】この場合、図10に示すように、図6の鍵入手のステップS2は、可視情報入手のステップS211と、その入手した可視情報を二次元処理により二次元ビットマップに変換して二次元情報を生成するステップS212と、秘密情報入手するステップS213と、それら二次元情報と秘密情報から署名鍵を生成するステップS214とで構成される。

【0067】このように署名鍵を秘密情報のみでなく可視情報（二次元情報）にも基づいて作成することにより、その作成された署名鍵を用いて作成される署名情報のユニーク性が更に高められる。

【0068】尚、この第3例における統合情報の生成にあたっては、署名を行なう前にコンテンツ情報に二次元情報を組み込むことにより二次元情報が組み込まれたコンテンツ情報を作成し、その二次元情報が組み込まれたコンテンツ情報に署名することにより得られる署名情報と、その二次元情報が組み込まれたコンテンツ情報とを統合してもよく、あるいは、二次元情報を組み込む前のコンテンツ情報に署名を行ない、その署名により生成された署名情報と、コンテンツ情報と、二次元情報とを統合してもよい。

【0069】図11は、図9、図10を参照して説明した第3例の具体例を示す模式図である。図10との相違点について説明する。

【0070】この図11には、手書き入力装置31が示されており、ユーザがこの手書き入力装置31を用いて自分のサインを入力する。するとそのサインを可視情報としてその可視情報について二次元処理が行なわれる。その他の点は、図9、図10を参照して説明したとおりである。

【0071】この場合、統合情報20として、コンテンツ情報20aと署名情報20bとの外に二次元情報20cも一体的に統合された統合情報が生成される。

【0072】図12は、図9、図10を参照して説明した第3例のもう1つの具体例を示す模式図である。

【0073】この図12には、二次元読み取り装置32が示されており、ユーザは、自分の印鑑をその二次読み取り装置32に押印する動作を行なう。そうするとその

二次元読み取り装置32はその印影を読み取ってその印影が可視情報として入力される。その後の処理は図11の場合と同様である。

【0074】このように、可視情報として手書きサインや印影を使用すると、従来から行なわれてきた手書きサイン認証や捺印認証と親和性のある署名認証を行なうことができる。

【0075】図13は、統合情報生成処理の第4例を示す模式図、図14はその第4例を実現するための、図6に示すフローチャートへの追加部分を示す部分フローチャートである。

【0076】図13における、図5に示す第1例との相違点は、付加情報入手し、コンテンツ情報に付加情報を付加した情報を署名鍵で署名する点である。

【0077】この場合、図6に示すフローチャート中のコンテンツ情報入手のステップ（ステップS1）と鍵入手のステップ（ステップS2）との間P1に、図14に示す付加情報入手のステップ（ステップS5）が挿入される。また、この場合、図6の統合処理のステップ（ステップS4）では、コンテンツ情報20aと署名情報20bとさらにその付加情報20dとが統合されて統合情報20が生成される。

【0078】ここで、付加情報は、例えば時刻情報であってもよく、上述のサインや印影等の可視情報（二次元情報）であってもよく、上述の秘密情報に類した情報であってもよい。

【0079】このようにコンテンツ情報に付加情報を付加して署名することにより、後の処理でその付加情報の有効利用を図ることができる。

【0080】図15は、統合情報生成処理の第5例を示す構成図、図16はその第5例を実現するための、図6に示すフローチャートへの追加部分を示す部分フローチャートである。

【0081】図15における、図5に示す第1例との相違点は、コンテンツ情報に時刻情報が付加されてその時刻情報が付加されたコンテンツ情報が生成され、その時刻情報を含むコンテンツ情報に署名処理が行なわれる。この場合、図6に示すフローチャート中の、コンテンツ情報入手のステップ（ステップS1）と鍵入手のステップ（ステップS2）との間P1に、図15に示す時刻情報入手のステップ（ステップS6）が挿入される。

【0082】ここで、この時刻情報は、コンテンツ情報が作成された時点の時刻を表わす時刻情報であってもよくコンテンツ情報に署名を行なう時点の時刻情報であってもよい。

【0083】このように時刻情報を付加することにより生成された、時刻情報を含むコンテンツ情報に署名し、その署名により得られた署名情報と、時刻情報を含むコンテンツ情報とを統合することにより、後の署名照合時等に時刻情報を運用することができる。

【0084】次に、統合情報中のコンテンツ情報が真正なものであるか否かの検証を行なう検証処理について説明する。

【0085】図17は、検証処理の第1例を示す模式図、図18はその検証処理の第1例を表わすフローチャートである。

【0086】ここでは、先ず統合情報20から署名情報とコンテンツ情報を分離する分離処理が行なわれる（ステップS7）。この分離処理は、図3に示す情報管理プログラム250の分離手段253に相当する。

【0087】次に、前述した統合情報生成処理において使用した署名鍵と同一の署名鍵を入手し（ステップS8）、その入手した署名鍵を用いて、その統合情報から分離されたコンテンツ情報10に署名処理を行ない検証用署名情報を生成する（ステップS9）。この検証用署名情報を作成するための署名処理は、図3に示す情報管理プログラム250の検証用署名手段254に相当する。

【0088】さらに、上記のように生成された検証用署名情報と、統合情報20から分離された署名情報とを比較照合してそれらの一致不一致を検出する比較処理が行なわれる（ステップS10）。この比較処理は、図3に示す情報管理プログラム250の比較手段225に相当する。

【0089】このように、実際に検証を行なうことができるように構成しておくことにより、コンテンツ情報に一体化された署名情報に信頼を置くことができ、ユーザに一層の安心感を与えることができる。

【0090】図19は、検証処理の第2例を示す模式図、図20は、その第2例を実現するための、図18に示すフローチャートからの変更部分を示す部分フローチャートである。

【0091】この場合、図20に示すように、鍵入手のステップ（ステップS8）は、秘密情報入手のステップS801と、その入手した秘密情報に基づいて署名鍵を生成するステップS802とで構成される。この図19、図20に示す第2例は、図7、図8を参照して説明した統合情報生成処理の第2例に対応しており、その統合情報生成処理の第2例で入手される秘密情報と同一の秘密情報が入手され、その入手した秘密情報に基づいて、同一のアルゴリズムにより、その統合情報生成処理の第2例で生成された署名鍵と同一の署名鍵が生成される。

【0092】図21は、検証処理の第3例を示す模式図、図22は、その第3例を実現するための、図18に示すフローチャートからの変更部分を示す部分フローチャートである。

【0093】この場合、図22に示すように、図18の鍵入手のステップS8は、可視情報入手のステップS811と、その入手した可視情報を二次元処理により二次

元ビットマップに変換して二次元情報を生成するステップS812と、秘密情報を入手するステップ813と、それら二次情報と秘密情報から署名鍵を生成するステップS814とで構成される。

【0094】この図21、図22に示す第3例は、図9、図10を参照して説明した統合情報生成処理の第3例に対応しており、その統合情報生成処理の第3例で入手される可視情報（二次元情報）および秘密情報と同一の可視情報（二次元情報）および秘密情報が入手され、その統合情報生成処理の第3例で生成される署名鍵と同一の署名鍵が生成される。

【0095】このように、秘密情報に基づいて、あるいは可視情報（二次元情報）と秘密情報とに基づいて、鍵情報を生成するシステムを構築すると、その鍵情報による署名により生成される署名情報のユニーク性を高めることができる。

【0096】図23は、検証処理の結果を示した模式図、図24は、図18に示す検証処理フローチャートに付加される部分フローチャートである。

【0097】図24に示す部分フローチャートは、図18に示すフローチャートの比較処理（ステップ10）の後の部分P2に挿入されるものであり、ここでは、比較処理（ステップS10）の結果、統合情報20から分離されたコンテンツ情報10に署名処理を行なうことにより生成された検証用署名情報と、統合情報20から分離された署名情報が一致した場合（ステップS11）にのみ、ユーザによるコンテンツ情報のアクセスが許可され（ステップS12）、不一致のときはそのアクセスは不許可となる（ステップS13）。ここでいうアクセスは、特定のアクセスにかぎられないが、例えば表示、プリント出力、送信等をいう。尚、このコンテンツ情報は署名情報とともに統合情報として一体化されており、したがってここでいうコンテンツ情報のアクセスは統合情報のアクセスを意味する。

【0098】このように、検証により真正なコンテンツ情報であることが確認された場合のみアクセスを許可することにより、改ざんあるいはデータエラーの可能性のあるコンテンツ情報へのアクセスを防止することができる。

【0099】

【発明の効果】以上、説明したように、本発明によればコンテンツ情報と署名情報が例えば表示画面上への表示あるいは用紙上へのプリント出力等の場合に、視覚的に一体化された統合情報に統合されているため、その統合情報として一体化された署名情報が、印影やサインと同様の役割りを果たし、ユーザに安心感を与えることができる。

【図面の簡単な説明】

【図1】本発明の情報管理装置の一実施形態を構成するパーソナルコンピュータの外観斜視図である。

【図 2】図 1 に外観を示すパーソナルコンピュータのハードウェア構成図である。

【図 3】CDROM に記憶された情報管理プログラムの一例を示す図である。

【図 4】本発明にいう情報管理プログラムが動作するもう 1 つの環境であるコンピュータネットワークを示す図である。

【図 5】統合情報生成処理の第 1 例を示す模式図である。

【図 6】統合情報生成処理の第 1 例を表わすフローチャートである。

【図 7】統合情報生成処理の第 2 例を示す模式図である。

【図 8】統合情報生成処理の第 2 例を実現するための、図 6 に示すフローチャートからの変更部分を示す部分フローチャートである。

【図 9】統合情報生成処理の第 3 例を示す模式図である。

【図 10】統合情報生成処理の第 3 例を実現するための、図 6 に示すフローチャートからの変更部分を示す部分フローチャートである。

【図 11】統合情報生成処理の第 3 例の具体例を示す模式図である。

【図 12】統合情報生成処理の第 3 例のもう 1 つの具体例を示す模式図である。

【図 13】統合情報生成処理の第 4 例を示す模式図である。

【図 14】統合情報生成処理の第 4 例を実現するための、図 6 に示すフローチャートへの追加部分を示す部分フローチャートである。

【図 15】統合情報生成処理の第 5 例を示す構成図である。

【図 16】統合情報生成処理の第 5 例を実現するための、図 6 に示すフローチャートへの追加部分を示す部分フローチャートである。

【図 17】検証処理の第 1 例を示す模式図である。

【図 18】検証処理の第 1 例を表わすフローチャートである。

【図 19】検証処理の第 2 例を示す模式図である。

【図 20】検証処理の第 2 例を実現するための、図 18 に示すフローチャートからの変更部分を示す部分フローチャートである。

【図 21】検証処理の第 3 例を示す模式図である。

【図 22】検証処理の第 3 例を実現するための、図 18 に示すフローチャートからの変更部分を示す部分フローチャートである。

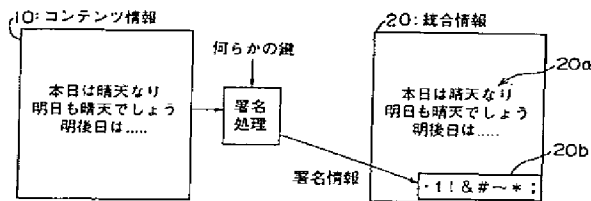
【図 23】検証処理の結果を示した模式図である。

【図 24】図 18 に示す検証処理フローチャートに付加される部分フローチャートである。

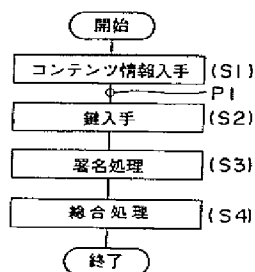
【符号の説明】

- 10 コンテンツ情報
- 20 情報処理プログラム
- 20a コンテンツ情報
- 20b 署名情報
- 20c 二次元情報
- 20d 付加情報
- 100 パーソナルコンピュータ
- 101 本体部
- 101a フロッピーディスク装填口
- 101b CDROM 装填口
- 102 CRT ディスプレイ
- 102a 表示画面
- 103 キーボード
- 104 マウス
- 210 CDROM
- 212 フロッピーディスク
- 221 中央演算処理装置 (CPU)
- 222 RAM
- 250 情報管理プログラム
- 251 署名手段
- 252 統合手段
- 253 分離手段
- 254 検証用署名手段
- 255 比較手段
- 300, 400 クライアントマシン
- 500 サーバマシン

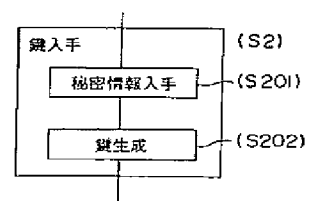
【図 5】



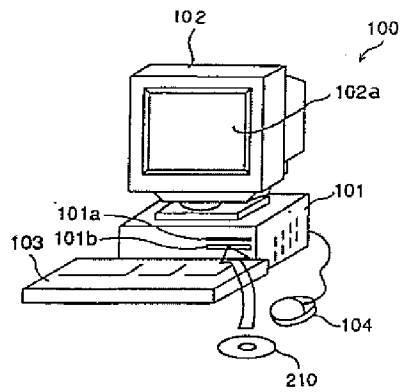
【図 6】



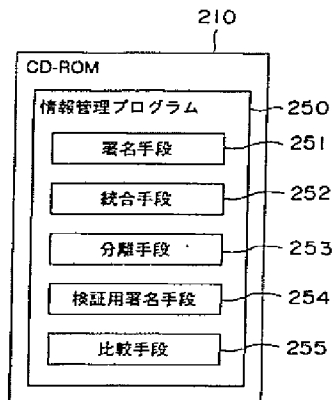
【図 8】



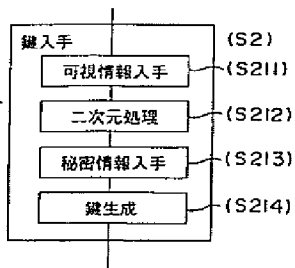
【図1】



【図3】



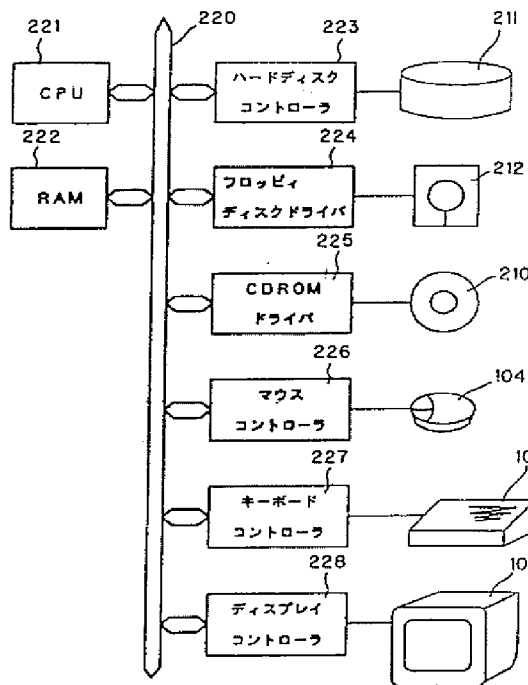
【図10】



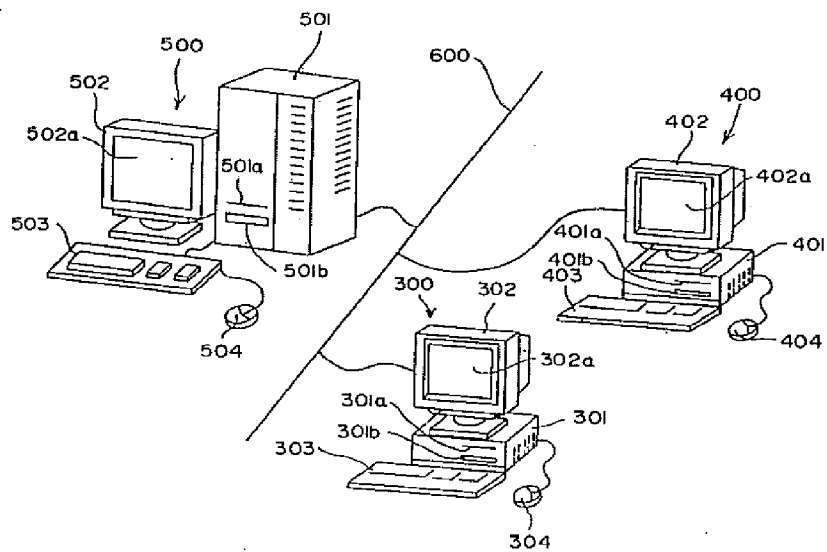
【図16】



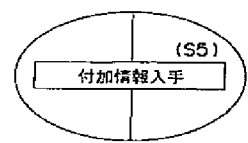
【図2】



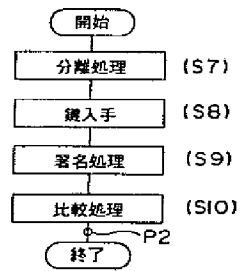
【図4】



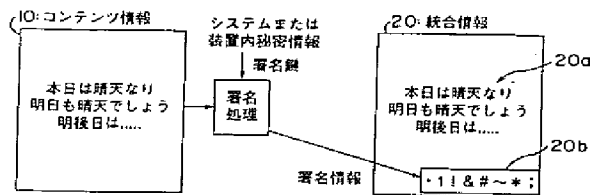
【図14】



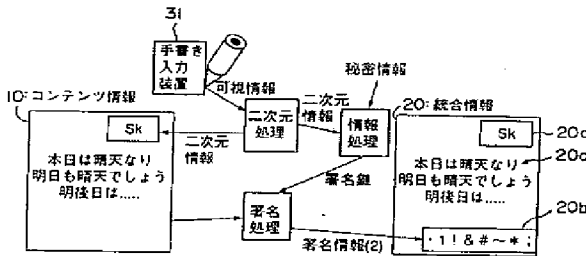
【図18】



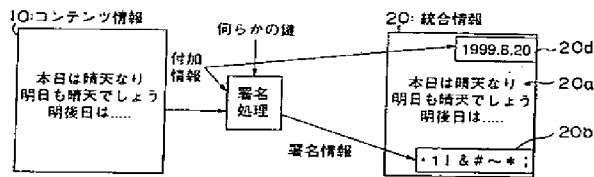
【図 7】



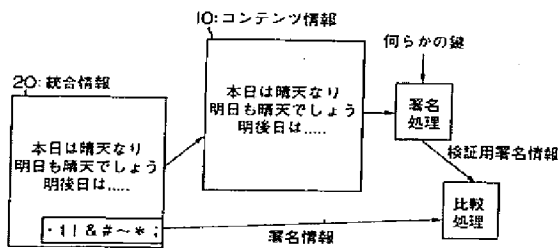
【図 11】



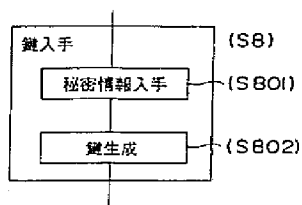
【図 13】



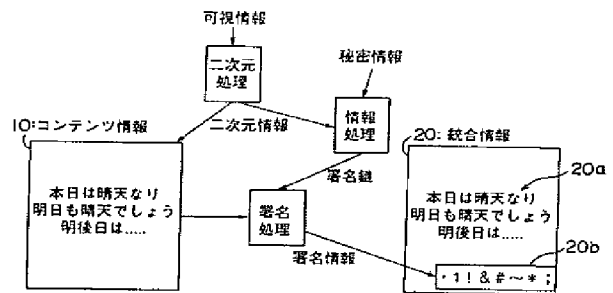
【図 17】



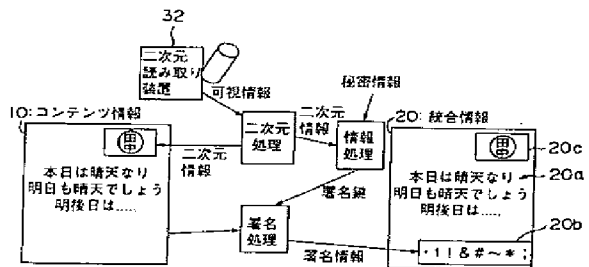
【図 20】



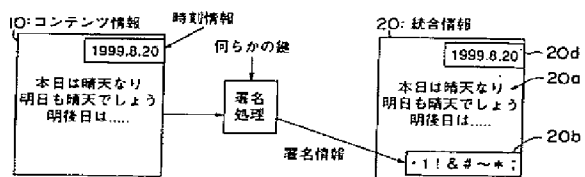
【図 9】



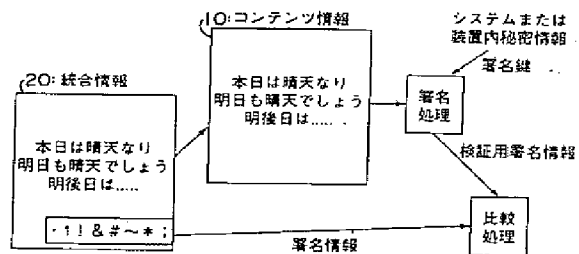
【図 12】



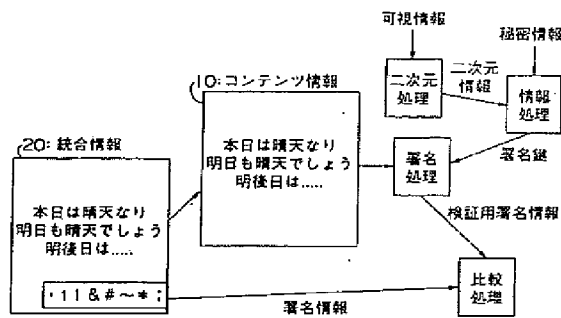
【図 15】



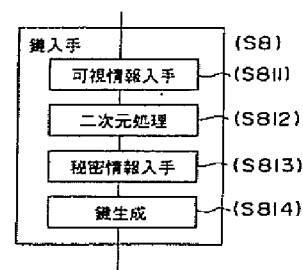
【図 19】



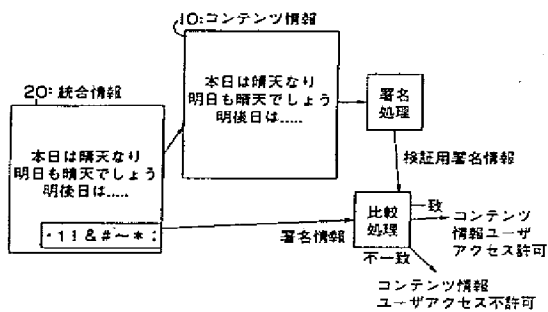
【図21】



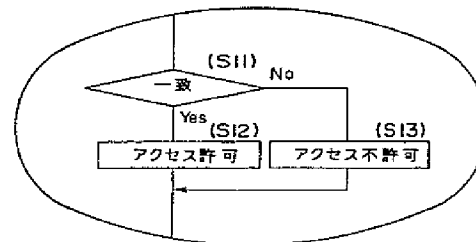
【図22】



【図23】



【図24】



フロントページの続き

(72) 発明者 秋山 良太
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内
(72) 発明者 佐々木 孝興
東京都港区芝浦4丁目15番33号 株式会社
富士通ビー・エス・シー内

Fターム(参考) 5B017 AA01 BA05 BA07 BB02 CA08
CA16
5C076 AA02 AA14 AA15 BA06
5J104 AA09 AA11 LA06 NA27
9A001 EE03 HZ28 JJ67 LL02